

WHAT IS CLAIMED IS:

1. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

receiving the message at the server from the sender,

5 transmitting from the server to the recipient the message and an attachment including the identity and address of the recipient and the identity of the sender and the time of the transmittal,

receiving the message and the attachment at the server from the recipient,

10 providing digital signatures of the message and the attachment at the server, and

authenticating to the recipient the message and the attachment at the server on the basis of the information received by the recipient from the server and on the basis of the digital signatures provided by the server

2. A method as set forth in claim 1 wherein the server creates digital fingerprints from the digital signatures and from the message and the attachment to authenticate the message and the attachment on the basis of the digital fingerprints.

3. A method as set forth in claim 1 wherein the attachment includes interim stations between the recipient and the server and wherein

20 the message and the attachment, and the digital signatures of the message and the attachment, are transmitted from the server to the sender to provide for a determination at the server for the sender of the authenticity of the message and the attachment

4. A method as set forth in claim 3 wherein the message and the attachment and the digital signatures of the message and the attachment are not retained at the sender when the message and the attachment and the digital signatures are transmitted from the server to the sender.

5 5. A method as set forth in claim 1 wherein the message and the attachment and the digital signatures of the message and the attachment are transmitted from the server to the sender.

6. A method as set forth in claim 5 wherein
the sender transmits to the server, to authenticate the message, the
10 information supplied by the server to the sender and wherein
the server operates upon the information from the sender to authenticate
the message.

7. A method as set forth in claim 5 wherein the message and the digital
signature of the message are discarded after the message and the digital signature are
15 transmitted by the server to the sender.

8. In a method of transmitting a message from a sender to a recipient
through a server displaced from the recipient, the steps at the server of:
receiving the message from the sender,
transmitting the message from the server to the recipient,
20 receiving the message at the server from the recipient,
providing at the server a digital signature of the message,
providing digital fingerprints of the message and the digital signature of
the message, and

comparing the digital fingerprints at the server to determine the authenticity of the message,

9. In a method as set forth in claim 8, the steps at the server of:
transmitting to the recipient the state of authenticity of the message on
5 the basis of the results of the comparison of the digital fingerprints.

10. In a method as set forth in claim 1, the steps at the server of:
transmitting to the server the message and the attachment, and
receiving from the sender the message and the attachment and the digital
signatures of the message and the attachment,

10 producing digital fingerprints of the message, the attachment and the
digital signatures, and

comparing the digital fingerprints relating to the message, and the digital
fingerprints relating to the attachment, to determine the authenticity of the message and
the attachment

15 11. In a method as set forth in claim 10, the steps at the server of:
disposing of the message and the attachment and the digital signatures of
the message and the attachment after transmitting this information to the sender.

12. In a method as set forth in claim 5, the steps at the server of:
providing at the server, at the same time as the reception of the message,
20 an attachment including the identity of the sender and the identity and address of the
server and the identity and address of the recipient and the time of transmission of the
message from the server to the recipient,

transmitting from the server to the recipient the attachment at the same time as the transmission of the message, and

receiving from the recipient at the server the message and the attachment,

providing digital fingerprints of the message, the attachment and the
5 digital signatures of the message and the attachment,

providing an indication of the authentication of the attachment on the basis of a comparison at the server of the digital fingerprints relating to the message and the digital fingerprints relating to the attachment

13. In a method as set forth in claim 12, the step at the server of:
10 transmitting from the server to the recipient an indication of the authenticity of the message on the basis of the comparison of the digital fingerprints relating to the message and the digital fingerprints relating to the attachment,

14. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the server of:

15 receiving the message at the server from the sender,

providing at the server, at the same time as the reception of the message at the server, an attachment including the identity of the sender and the identity and address of the recipient and the time of transmission of the message,

providing digital signatures of the message and the attachment at the
20 server,

sending the message and the attachment to the recipient,

receiving from the recipient the message and the attachment, and

determining the authenticity of the message and the attachment at the server from the message and the attachment at the server and the digital signatures at the server of the message and the attachment,

15. A method as set forth in claim 14 wherein

5 digital fingerprints are provided at the server of the message and the attachment and digital fingerprints are provided at the server of the digital signatures of the message and the attachment and wherein

a comparison is provided at the server of the digital fingerprints of the message and the digital signature of the message, and the attachment and the digital
10 signature of the attachment, to determine the authenticity of the message and the attachment.

16. A method as set forth in claim 15 wherein

the indications of the state of authenticity of the message and the attachment are transmitted from the server to the recipient and wherein

15 the message and the attachment and the digital signatures of the message and the attachment are discarded at the server when the indications of the authenticity of the message and the attachment are transmitted from the server to the recipient.

17. A method as set forth in claim 14 wherein

the message and the attachment and the digital signatures of the message
20 and the attachment are transmitted from the server to the sender and wherein

the server produces digital fingerprints of the message and the attachment and digital fingerprints of the digital signature of the message and the attachment and wherein

the server compares the digital fingerprints relating to the message, and the digital fingerprints relating to the attachment, to determine the authenticity of the message and the attachment.

18. A method as set forth in claim 17 wherein
5 the server transmits to the recipient the results of the comparison and wherein

the server discards the message and the attachment and the digital signatures of the message and the attachment when the server transmits the message and the attachment and the digital signature of the message and the attachment to the
10 recipient.

19. In a method as set forth in claim 1 wherein
the message is received at the server through the internet and wherein
the message and the digital signature of the message are transmitted to
the recipient through the internet.

15 20. In a method as set forth in claim 19 wherein
the state of authenticity of the message is transmitted through the internet
to the recipient.

21. In a method as set forth in claim 8 wherein
the message from the sender is received at the server through the internet
20 and wherein
the message is transmitted to the recipient through the internet.

22. In a method as set forth in claim 21 wherein
the state of authenticity of the message is transmitted from the server to
the recipient through the internet.

23. In a method as set forth in claim 14 wherein
5 the message is transmitted from the sender to the server through the
internet and wherein

the message and the attachment are transmitted from the server to the
recipient through the internet and wherein

10 the indication of the state of authenticity of the message and the
attachment are transmitted from the server to the recipient through the internet.

24. In a method of transmitting a message from a sender to a recipient
through a server displaced from the recipient, the steps at the server of:

receiving the message from the recipient at a web site providing at the
server for an indication of the authenticity of the message,

15 providing a compressed encrypted version of the message where the
compression is a particular compression and the encryption is a particular encryption,

decompressing the message in accordance with the particular
compression to provide a first digital fingerprint of the message,

20 decrypting the compressed encrypted version of the message in
accordance with the particular encryption to provide a second digital fingerprint of the
message, and

comparing the first and second digital fingerprints of the message to
determine the authenticity of the message.

26. In a method as set forth in claim 25, the steps at the server of:
receiving the message through the internet from the recipient, and
transmitting the results of the comparison of the first and second digital
fingerprints to the recipient through the internet.

- 5 27. In a method of transmitting a message from a sender to a recipient
through a server displaced from the recipient, the steps at the server of:
receiving the message from the recipient at a website providing in the
server for an indication of the authenticity of the message,
providing a compressed encrypted version of the message where the
10 compression is a particular compression and the encryption is a particular encryption,
receiving an attachment from the recipient at the website where the
reception of the attachment is at the same time as the reception of the message,
providing a compressed encrypted version of the message where the
compression is the particular compression and the encryption is the particular
15 encryption,
decompressing the message and the attachment in accordance with the
particular compression to provide first digital fingerprints of the message and the
attachment,
decrypting the compressed encrypted versions of the message and the
20 attachment in accordance with the particular encryption to provide second digital
fingerprints of the message and the attachment, and

comparing the first and second digital fingerprints of the message, and the first and second digital fingerprints of the attachment, to determine the authenticity of the message and of the attachment.

28. In a method as set forth in claim 27, the step at the server of:
5 transmitting to the recipient the results of the comparison of the first and second digital fingerprints of the message and the first and second digital fingerprints of the attachment.

29. In a method as set forth in claim 27 wherein
the attachment includes the identity of the sender and the identity and the
10 address of the server and the identity and address of the recipient and the time of transmission of the message from the server to the recipient,

30. In a method as set forth in claim 27, including the steps at the server of:
receiving the message and the attachment through the internet from the
recipient, and
15 transmitting the results of the comparison of the first and second digital fingerprints of the message, and the comparison of the first and second digital fingerprints of the attachment, to the recipient through the internet.

31. In a method as set forth in claim 28, the steps at the server of:
transmitting to the recipient through the internet the results of the
20 comparison of the first and second digital fingerprints of the message and the first and second digital fingerprints of the attachment,

32. In a method as set forth in claim 27 wherein
the attachment includes the identity of the sender and the identity and the
address of the server and the identity and address of the recipient and the time of
transmission of the message from the server to the recipient.

5 33. In a method of transmitting a message from a sender through a server
displaced from the recipient, the steps at the server of:

receiving the message and an attachment from the recipient at a website
providing at the server for an indication of the authenticity of the message,

10 providing at the server for a compressed encrypted version of the
combination of the message and the attachment where the compression is a particular
compression and the encryption is a particular compression,

decompressing the compressed encrypted version of the combination of
the message and the attachment in accordance with the particular compression to
provide a first digital fingerprint of the combination of the message and the attachment,

15 decrypting the compressed encrypted version of the combination of the
message and the attachment in accordance with the particular encryption to provide a
second digital fingerprint of the combination of the message and the attachment, and

comparing the first and second digital fingerprints to determine the
authenticity of the message and the attachment.

20 34. In a method as set forth in claim 33, the step at the server of:
transmitting to the recipient the results of the comparison of the first and
second digital fingerprints.

35. In a method as set forth in claim 34, the steps at the server of:
receiving the message and the attachment, and the compressed encrypted
version of the combination of the message and the attachment, through the internet,
and

5 transmitting the results of the comparison of the first and second digital
fingerprints to the recipient through the internet.

36. In a method as set forth in claim 33 wherein
the attachment includes the identity of the sender and the identity and the
address of the server and the identity and address of the recipient and the time of the
10 transmittal of the message to the recipient.

37. In a method as set forth in claim 35, the steps at the server of:
transmitting to the recipient the results of the comparison of the first and
second digital fingerprints and wherein
the attachment includes the identity of the sender and the identity and the
15 address of the server and the identity and address of the recipient and the time of the
transmittal from the server to the recipient.

38. In a method of transmitting a message and an attachment from
a sender to a recipient through a server displaced from the recipient, including the steps
at the server of
20 identifying the sender,
hashing the attachments,
stripping the message of the attachments,

hashing the identification of the sender, the hashed attachments and
the message to form a hashed string,

hashing the hashed string,

encrypting the hashed string after the hashing of the hashed string, and

5 digitally sealing the encrypted hash of the hashed string.

39. In a method as set forth in claim 38, the steps of:

adding the message to the encrypted hash of the hashed string, and

transmitting the message and the encrypted hash of the hashed string to
the recipient.

10 40. In a method of transmitting a message and an attachment from a
sender through a server displaced from the recipient, the steps at the server of:

identifying the sender,

providing the attachment and the message stripped of the attachment,

providing a string formed from the identification of the sender, the

15 attachment and the message stripped of the attachment, and

hashing the strip.

41. In a method as set forth in claim 40, the steps of:

hashing the string, and

encrypting the hash of the hashed string.

42. In a method as set forth in claim 41, the steps of
digitally sealing the encrypted hash of the hashed string,
attaching the message to the encrypted hash of the hashed string, and
5 sending to the recipient the message and the encrypted hash of the
hashed string.

43. In a method of authenticating at a recipient a message and an
attachment transmitted from a sender to the recipient through a server displaced from
the recipient, the steps of:

10 providing at the recipient a string comprising a compressed and
encrypted embedded hash of a string including an identification of the sender, the
message and a hash of the attachment,

decompressing the string,

decrypting the decompressed string,

15 decrypting the decompressed string,

hashing the string less the hash of the string,

comparing the hash produced in the string and the embedded hash, and

using the results of the comparison to indicate to the recipient the
authenticity of the message and the attachment.

44. In a method as set forth in claim 43, the steps of:

separating the attachment from the message,

hashing the separated attachment,

comparing the hashed separated attachment and the hashed attachment in

5 the string, and

using the results of the comparison provided in the previous step to

indicate the authenticity of the message and the attachment.

45. In a method as set forth in claim 44, the step of:

recovering the message and the attachment and transmitting the

10 recovered message and attachment to the recipient with the indication of their
authenticity.

46. In a method of authenticating at a recipient a message and an attachment

transmitted from a sender to the recipient,

providing an attachment,

15 providing at the recipient on encryptment of a hashed string including
information relating to the identification of the sender, the attachment and the message
stripped of the attachment,

decrypting the encrypted hash of the hashed string,

decompressing the hash from the hashed string,

20 separating the hash from the string,

forming a hash from the information relating to the identification of the sender, the attachment and the message stripped of the attachment,

comparing the hash separated from the string and the hash formed from the information in the string, and

5 using the results of the comparison to indicate to the recipient the authenticity of the message and the attachment.

47. In a method as set forth in claim 46,

separating the attachment received at the server from the recipient from the other information received at the server from the recipient,

10 hashing the separated attachment to form a first hash,

the information relating in the string to the attachment including a hash of the attachment,

separating the hash of the attachment from the string to form a second hash,

15 comparing the first and second hashes, and

using the results of the comparison to indicate to the recipient the authenticity of the message and the attachment received at the recipient.